Note di Matematica
Note Mat. **34** (2014) no. 2, 23–40.
ISSN 1123-2536, e-ISSN 1590-0932
doi:10.1285/i15900932v34n2p23

On the structure of involutions and symmetric spaces of dihedral groups

K. K. A. Cunningham
Southern University and A&M College katrina_cunningham@subr.edu

Tom Edgar
Pacific Lutheran University edgartj@plu.edu

A.G. Helminck
North Carolina State University loek@math.ncsu.edu

B.F. Jones
Galois Inc. benjaminfjones@gmail.com

H. Oh
Bennett College hoh@bennett.edu

R. Schwell
Central Connecticut State University schwellrac@ccsu.edu

J. F. Vasquez
The University of Scranton jennifer.vasquez@scranton.edu

Received: 21.8.2013; accepted: 8.3.2014.

Abstract. We initiate the study of analogues of symmetric spaces for finite groups, with the current work focusing on the family of finite dihedral groups. In particular, we investigate the structure of the automorphism group, characterize the involutions within the automorphism group, and determine the fixed-point subgroup and symmetric space of each automorphism.

Keywords: dihedral groups, symmetric spaces, involutions, automorphisms.

MSC 2000 classification: Primary: 20F28; Secondary: 53C35, 20C99

Introduction

Let G be a group and $\theta \in \mathrm{Aut}(G)$ such that $\theta^m = \mathsf{id}$. We then define the following two sets:

$$H = G^\theta = \{g \in G \mid \theta(g) = g\}$$
$$Q = \{g \in G \mid g = x\theta(x)^{-1} \text{ for some } x \in G\}.$$

The set H is the fixed-point subgroup corresponding to θ and Q is known as a *Generalized Symmetric Space*. If θ is an involution and G is a real reductive

Lie group, then the set Q is a reductive symmetric space. If G is a reductive algebraic group defined over an algebraically closed field k, then Q is also known as a symmetric variety and if G is defined over a non-algebraically closed field k, then the set $Q_{\mathsf{k}} := \{x\theta(x)^{-1} \mid x \in G_{\mathsf{k}}\}$ is called a symmetric k-variety. Here G_{k} denotes the set of k-rational points of G. Reductive symmetric spaces and symmetric k-varieties are well known for their role in many areas of mathematics. They are probably best known for their fundamental role in representation theory [5]. The generalized symmetric spaces as defined above are of importance in a number of areas as well, including group theory, number theory, and representation theory.

One of the first questions that arises in the study of these generalized symmetric spaces is the classification of the automorphisms up to isomorphy, where isomorphy is given by either conjugation by inner automorphisms, outer automorphisms, or both depending on which makes the most sense.

To analyze the structure of these generalized symmetric spaces one looks at orbits of both the group itself and the fixed-point subgroup. Both G and H act on Q by θ-twisted conjugation which we denote by $*$. For $g \in G$ and $q \in Q$ we have

$$g * q = gq\theta(g)^{-1}.$$

Since H is the set of fixed points, this action is simply conjugation when restricted to H. Also, if θ is an involution, then Q is in bijective correspondence with G/H under the map $\tau : G \to Q$ given by $\tau(g) = g\theta(g)^{-1}$.

We are interested in classifying G and H orbits in Q and describing how the G-orbits decompose into H-orbits. In particular, if θ is an involution it is known that set of H-orbits, denoted $H\backslash Q$, corresponds to the collection of double cosets $H\backslash G/H$. These orbits and double cosets play an important role in representation theory [5].

This paper focuses on understanding the structures described above when G is the dihedral group of order $2n$, that is $G = D_n$. In particular, we determine the sets H and Q explicitly, provide a procedure for enumerating the involutions, and give a closed formula for counting the equivalence classes of involutions of D_n.

The paper is organized as follows. In Section 1, we introduce the necessary preliminaries including our choices for notation and the well known description of the automorphism group of D_n as well as some relevant examples. In Section 2, we investigate and describe all the automorphisms of D_n of a fixed order. We recall the notion of equivalence of automorphisms and give simple conditions for two automorphisms of D_n to be equivalent. Furthermore, we provide a formula for computing the total number of equivalence classes of automorphisms of a fixed order. In Section 3, we give full descriptions of the sets H and Q as well as

the orbits of Q under the action by H and by G. In Section 4, we find stronger results for the involutions in the automorphism group. Our main technical result is to partition the set of involutions in such a way that there are at most two distinct equivalence classes of involutions in each piece of the partition (cf. Theorem 5). We also show that in the involution case, Q is always a subgroup of G, and we describe the subgroup structure of Q. Furthermore, we introduce the set of twisted involutions, R, and give a characterization of this set and its relation to the generalized symmetric space. Using our results on involutions of D_n, we provide a counterexample to a standard theorem on equivalence of involutions which holds for algebraic groups. Finally, in Section 5, we complete the discussion by applying our methods to the infinite dihedral group in order to understand the automorphisms of finite order, as well as H and Q in that context.

1 Preliminaries

1.1 The Dihedral Group and its Automorphism Group

Throughout the paper we denote by D_n the group of symmetries of the regular n-gon, and we only consider the case $n \geq 3$. More specifically, D_n is a finitely generated group given by the presentation

$$D_n = \langle r, s \mid r^n = s^2 = 1,\ sr = r^{-1}s \rangle.$$

We use this presentation, instead of the presentation as a Coxeter group (see [2, Example 1.2.7], [6, §1.1, §4.2], [3, §1.2]), because it is convenient for describing the automorphism group of D_n. From the presentation it is clear that

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}$$

and we say that an element of D_n is presented in *normal form* if it is written as $r^k s^m$ for some integers $0 \leq k < n$ and $s \in \{0, 1\}$.

Throughout the paper, $\mathbb{Z}_n$ denotes the additive group of integers modulo n and U_n denotes the multiplicative group of units of $\mathbb{Z}_n$. Recall that $a \in U_n$ if and only if $\gcd(\dot{a}, n) = 1$ for any representative integer $\dot{a}$ of $a \in \mathbb{Z}_n$.

We also find it useful to have terminology for the k-th roots of unity in $\mathbb{Z}_n$ (equivalently in U_n), which can be described by

$$\mathcal{R}_n^k := \{a \in U_n \mid a^k = 1\}.$$

The automorphism group of D_n is well known (see [9, Theorem A]) and is described in the following lemma.

Lemma 1. *Let $n \geq 3$. The automorphism group of D_n is isomorphic to the group of affine linear transformations of $\mathbb{Z}_n$:*

$$\mathrm{Aut}(D_n) \cong \mathrm{Aff}(\mathbb{Z}_n) = \{ax + b : \mathbb{Z}_n \to \mathbb{Z}_n \mid a \in U_n, b \in \mathbb{Z}_n\}$$

and the action of $ax + b$ on elements of D_n in normal form is given by:

$$(ax + b).(r^k s^m) = r^{ak+bm} s^m.$$

Proof. Note that every automorphism of D_n is determined by its action on r and s and can then be described by how it acts on the normal form of the elements. So, if θ is an automorphism, then $\theta(r)$ must have order n since r does; as such, $\theta(r) = r^a$ where $a \in U_n$. Similarly, $\theta(s) = r^b s$ for some $0 \leq b < n$ since s has order 2 and the only elements of D_n of order 2 are of the form $r^b s$. Putting these together, we see that if $\theta \in \mathrm{Aut}(D_n)$, then for any $r^k s^m \in D_n$ we must have $\theta(r^k s^m) = r^{ak+bm} s^m$. There is now a clear map from $\mathrm{Aut}(D_n) \to \mathrm{Aff}(\mathbb{Z}_n)$ and it is easily checked to be an isomorphism. QED

Throughout the paper we abuse notation and write $\theta = ax + b$ for elements $\theta \in \mathrm{Aut}(D_n)$ according to Lemma 1.

We now see how the inner automorphisms fit in the framework of Lemma 1. Suppose $\theta = \mathrm{conj}(g)$, conjugation by an element $g \in D_n$. If $\theta = ax + b$ corresponds to $g = r^k$, then it is easy to see that $a = 1$ and $b = 2k$ (in U_n and $\mathbb{Z}_n$ respectively). On the other hand, if $g = r^k s$, then we have $a = n - 1$ and $b = 2k$. In particular, if $\theta = ax + b$ corresponds to an inner automorphism then $a \equiv \pm 1 \pmod{n}$. Also, we see that when n is even, there are n distinct inner automorphisms (corresponding to $a \equiv \pm 1 \pmod{n}$ and $b \in \langle 2 \rangle \leq \mathbb{Z}_n$, and when n is odd, there are $2n$ distinct inner automorphisms corresponding to $a \equiv \pm 1 \pmod{n}$ and $b \in \langle 2 \rangle = \mathbb{Z}_n$. Recall that the group of inner automorphisms is isomorphic to D_n modulo the center of D_n. Since the center of D_n is trivial when n is odd and has order 2 when n is even, we expect these two different cases.

When n is even, it is well known from the theory of Coxeter groups that one of the outer automorphisms of D_n corresponds to the interchanging of the two conjugacy classes of reflections; this is known as the diagram automorphism (cf. [3, §4.2]). This automorphism is given by $\theta = ax + b$ where $a = n - 1$ and $b = n - 1$. When n is odd, this automorphism is inner as shown in the previous paragraph.

2 Automorphisms of D_n

In this section we describe the action of the automorphism group on D_n ($n \geq 3$), we characterize the automorphisms of fixed order, and we discuss the

notion of equivalent automorphisms.

For any $c \in \mathbb{Z}_n$, we define $\mathrm{ZDiv_n}(c) = \{y \in \mathbb{Z}_n \mid cy \equiv 0 \bmod n\}$. It is trivial to check that $\mathrm{ZDiv_n}(c)$ is a subgroup of $\mathbb{Z}_n$. In particular, $\mathrm{ZDiv_n}(c) = \ker \pi_c$ where $\pi_c : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $\pi_c(x) = cx$. Note that $\mathrm{im}(\pi_c) = \langle c \rangle$ and so $|\mathrm{im}(\pi_c)| = \frac{n}{\gcd(c,n)}$. Since $\mathrm{im}(\pi_c) \cong \mathbb{Z}_n/\ker(\pi_c) \cong \mathbb{Z}_n/\mathrm{ZDiv_n}(c)$, it follows that $|\mathrm{ZDiv_n}(c)| = \gcd(c, n)$. We use this notation to describe the automorphisms of finite order dividing k.

Proposition 1. *Let $k \geq 1$ be an integer and $\theta \in \mathrm{Aut}(D_n)$ with $\theta = ax + b$. Then $\theta^k = \mathsf{id}$ if and only if $a \in \mathcal{R}_n^k$ and $b \in \mathrm{ZDiv_n}(a^{k-1} + a^{k-2} + \cdots + a + 1)$.*

Proof. Straightforward computation in $\mathrm{Aut}(D_n)$ gives us that

$$\theta^k = a^k x + (a^{k-1} + a^{k-2} + \cdots + a + 1)b$$

Since we have identified the identity automorphism with $x \in \mathrm{Aff}(\mathbb{Z}_n)$ the following two equations hold:

$$\begin{aligned} a^k &\equiv 1 \pmod{n} \\ (a^{k-1} + a^{k-2} + \cdots + 1)b &\equiv 0 \pmod{n}. \end{aligned} \tag{1}$$

In the notation described above, these are evidently equivalent to $a \in \mathcal{R}_n^k$ and $b \in \mathrm{ZDiv_n}(a^{k-1} + a^{k-2} + \cdots + a + 1)$. QED

In what follows, we let $\mathrm{Aut}_k(D_n) = \{\theta \in \mathrm{Aut}(D_n) \mid \theta^k = \mathsf{id}\} \subseteq \mathrm{Aut}(D_n)$. Also, for the remainder of the paper, we note that $\gcd(0, n) = n$ for all natural numbers n.

Proposition 2. *For any $n \geq 3$ and $k \geq 1$, we have*

$$|\mathrm{Aut}_k(D_n)| = \sum_{a \in \mathcal{R}_n^k} \gcd(a^{k-1} + a^{k-2} + \cdots + a + 1, n).$$

Proof. This follows from Proposition 1: for any $a \in \mathcal{R}_n^k$ there are

$$|\mathrm{ZDiv_n}(a^{k-1} + a^{k-2} + \cdots + 1)| = \gcd(a^{k-1} + a^{k-2} + \cdots + 1, n)$$

elements b such that $(a^{k-1} + a^{k-2} + \cdots + 1)b \equiv 0 \pmod{n}$, and every automorphism $\theta \in \mathrm{Aut}_k(D_n)$ must be of this form. QED

Definition 1. Let $\theta_1, \theta_2 \in \mathrm{Aut}(D_n)$. We say that θ_1 is *equivalent* to θ_2 and write $\theta_1 \sim \theta_2$ if and only if they are conjugate to each other, i.e. if there is $\sigma \in \mathrm{Aut}(D_n)$ with $\sigma\theta_1\sigma^{-1} = \theta_2$. For any $\theta \in \mathrm{Aut}(D_n)$ we let $\overline{\theta} = \{\sigma \in \mathrm{Aut}(D_n) \mid \theta \sim \sigma\}$ be the equivalence class of θ.

Remark 1. This definition of equivalence is broad (since we allow conjugation by any automorphism, not just the inner ones), but still useful. In particular, it simplifies the statement of the following proposition and it allows us not to worry about the parity of n in several places.

Proposition 3. *Let $\theta_1 = ax + b \in \mathrm{Aut}(D_n)$ and $\theta_2 = cx + d \in \mathrm{Aut}(D_n)$. Then $\theta_1 \sim \theta_2$ if and only if $a = c$ and $fb - d \in \langle a - 1\rangle \leq \mathbb{Z}_n$ for some $f \in U_n$.*

Proof. Suppose that $\sigma = fx + g \in \mathrm{Aut}(D_n)$ (so that $f \in U_n$ and $g \in \mathbb{Z}_n$). It is easily checked that $\sigma^{-1} = f^{-1}x - f^{-1}g$ where $f^{-1} \in \mathbb{Z}_n$ since $f \in U_n$. Then $\sigma\theta_1\sigma^{-1} = \tau$, where $\tau = f(a(f^{-1}x - f^{-1}g) + b) + g = ax + fb - g(a - 1)$. Thus, we can conclude that $\sigma\theta_1\sigma^{-1} = \theta_2$ if and only if $a = c$ and $fb - g(a - 1) = d$. The second equation can be written as $fb - d = g(a - 1)$, and thus $fb - d \in \langle a - 1\rangle$. QED

The previous proposition allows us to describe the conjugacy classes of automorphisms with order dividing k.

Proposition 4. *Suppose n is fixed and let $k \geq 1$.*

(1) For any $a \in \mathcal{R}_n^k$, $\langle a - 1\rangle \leq \mathrm{ZDiv_n}(a^{k-1} + a^{k-2} + \cdots + a + 1)$.

(2) For any $a \in \mathcal{R}_n^k$, U_n acts on $\mathrm{ZDiv_n}(a^{k-1} + a^{k-2} + \cdots + a + 1)/\langle a - 1\rangle$.

(3) The set $\mathrm{Aut}_k(D_n)$ is partitioned into equivalence classes in which the classes are indexed by pairs (a, B) where $a \in \mathcal{R}_n^k$ and B is an orbit of U_n on $\mathrm{ZDiv_n}(a^{k-1} + a^{k-2} + \cdots + a + 1)/\langle a - 1\rangle$.

Proof. Part (1) is trivial since $(a - 1)(a^{k-1} + a^{k-2} + \cdots + a + 1) = a^k - 1 \equiv 0$. For part (2), we simply recognize that $U_n = \mathrm{Aut}(\mathbb{Z}_n)$ acts on $\mathbb{Z}_n$ by multiplication and since every subgroup is cyclic, U_n must stabilize the subgroups of $\mathbb{Z}_n$. Finally, part (3) is simply Proposition 3 in terms of the U_n-action on $\mathrm{ZDiv_n}(a^{k-1} + a^{k-2} + \cdots + a + 1)/\langle a - 1\rangle$. QED

Proposition 3 and Proposition 4 help us determine the total number of equivalence classes of finite order automorphisms. For fixed $a \in \mathcal{R}_n^k$, we want to compute

$$N_a := |\{\overline{\theta} \mid \theta = ax + b \in \mathrm{Aut}_k(D_n)\}|. \tag{2}$$

By to Proposition 4, given $a \in \mathcal{R}_n^k$, computing N_a amounts to counting the number of orbits of the U_n-action on $\mathrm{ZDiv_n}(a^{k-1} + a^{k-2} + \cdots + a + 1)/\langle a - 1\rangle$.

Theorem 1. *Let n be fixed and let $a \in \mathcal{R}_n^k$. Then, the number of orbits of U_n on $\mathrm{ZDiv_n}(a^{k-1} + a^{k-2} + \cdots + a + 1)/\langle a - 1\rangle$ is equal to the number of divisors of*

$$\frac{\gcd(a - 1, n)\gcd(a^{k-1} + a^{k-2} + \cdots + a + 1, n)}{n}.$$

Proof. The U_n-orbits on $\mathbb{Z}_n$ are indexed by the subgroups of $\mathbb{Z}_n$. Thus, the U_n-orbits on $\mathrm{ZDiv_n}(a^{k-1}+a^{k-2}+\cdots+a+1)/\langle a-1\rangle$ are indexed by subgroups $L \leq \mathbb{Z}_n$ such that $\langle a-1\rangle \leq L \leq \mathrm{ZDiv_n}(a^{k-1}+a^{k-2}+\cdots+a+1)$. It is well known that the subgroup lattice of $\mathbb{Z}_n$ is isomorphic to the divisor lattice of n. Under the previous lattice isomorphism, the subgroup $\langle a-1\rangle$ corresponds to the divisor $\gcd(a-1,n)$ and the subgroup $\mathrm{ZDiv_n}(a^{k-1}+a^{k-2}+\cdots+a+1)$ corresponds to the divisor

$$\frac{n}{\gcd(a^{k-1}+\cdots+a+1,n)};$$

the subgroups between these groups correspond to the divisors of n between $\gcd(a-1,n)$ and $\frac{n}{\gcd(a^{k-1}+\cdots+a+a,n)}$ in the divisor lattice. Finally, it is known that this sub-lattice of the divisors of n is isomorphic to the divisor lattice of

$$\frac{\gcd(a-1,n)}{\frac{n}{\gcd(a^{k-1}+\cdots+a+1,n)}} = \frac{\gcd(a-1,n)\gcd(a^{k-1}+a^{k-2}+\cdots+a+1,n)}{n}.$$

QED

Given a specific n, Theorem 1 and Proposition 4 allow us to compute all the equivalence classes of automorphisms of order k using any standard computer algebra package. In Section 4, we investigate N_a when $a \in \mathcal{R}_n^2$ (i.e. θ is an involution).

3 Fixed-point Groups and Symmetric Spaces of Automorphisms

Recall from the introduction that we are interested in two different subsets of a group G. Namely, given an automorphism, θ, we want to compute

$$H_\theta = G^\theta = \{x \in G \mid \theta(x) = x\} \text{ and}$$
$$Q_\theta = \{g \in G \mid g = x\theta(x)^{-1} \text{ for some } x \in G\}.$$

When θ is understood to be fixed, we drop the subscript from our notation. The following theorem characterizes these spaces in the case of dihedral groups.

Theorem 2. *Let $G = D_n$ and $\theta = ax+b \in \mathrm{Aut}(D_n)$ be of finite order, and let H and Q be as defined above. Then*

$$H = \{r^k \mid k(a-1) \equiv 0 \pmod n\} \cup \{r^k s \mid k(a-1) \equiv -b \pmod n\} \text{ and}$$
$$Q = \{r^k \mid k \in \langle a-1\rangle \cup (-b + \langle a-1\rangle)\},$$

where $\langle a-1\rangle \leq \mathbb{Z}_n$.

Proof. Recall that if $\theta = ax + b \in \mathrm{Aut}(D_n)$, then the formula $\theta(r^k s^m) = r^{ak+bm}s^m$ provides the full description of the action of θ. All of the results of the theorem arise from the definitions of H and Q using the action of θ described above. Suppose $\theta(r^k) = r^k$, then $r^{ak} = r^k$ and so $ak - k \equiv 0 \pmod{n}$, i.e. $k(a-1) \equiv 0 \pmod{n}$. On the other hand, if $\theta(r^k s) = r^k s$, then $r^{ak+b}s = r^k s$ and so $ak - k + b \equiv 0 \pmod{n}$, i.e. $k(a-1) \equiv -b \pmod{n}$. Thus, we obtain the desired description of H.

Using the same computations as above, we see that $r^k\theta(r^k)^{-1} = r^k r^{-ak} = r^{-k(a-1)}$ and $r^k s\theta(r^k s)^{-1} = r^k s r^{ak+b}s = r^k r^{-(ak+b)}ss = r^{-k(a-1)-b}$. Hence, the characterization of Q is obtained as well. QED

Using the descriptions of H and Q, we obtain further results as well.

Corollary 1. *Let $\theta = ax+b \in \mathrm{Aut}(D_n)$ be of finite order and $\langle a-1\rangle \leq \mathbb{Z}_n$. Then*

(1) If $b \notin \langle a-1\rangle$, then $H \cong \mathrm{ZDiv_n}(a-1)$ is cyclic.

(2) If $b \in \langle a-1\rangle$, then $H \cong \mathrm{ZDiv_n}(a-1) \rtimes \mathbb{Z}_2$ is dihedral.

Corollary 2. *Let n, k, and $\theta = ax + b \in \mathrm{Aut}_k(D_n)$ be fixed. If $b \in \langle a-1\rangle$ then Q is a subgroup of D_n and $Q \cong \langle a-1\rangle$.*

We will show in the next section that when θ is an involution, Q is always a subgroup of D_n (see Corollary 6).

Corollary 3. *Let $\theta = ax + b \in \mathrm{Aut}(D_n)$ be a fixed automorphism. If $b \notin \langle a-1\rangle \leq \mathbb{Z}_n$, then $HQ \neq D_n$. If $b \in \langle a-1\rangle$, then the following are equivalent*

(1) $HQ = D_n$

(2) $H \cap Q = \{1\}$ in D_n, and

(3) $\gcd(a-1, n)$ is relatively prime to $\frac{n}{\gcd(a-1,n)}$.

Proof. From Corollary 1 and the fact that $Q \subseteq \langle r\rangle$, we see that if $b \notin \langle a-1\rangle$ then $HQ \subseteq \langle r\rangle \neq D_n$. If $b \in \langle a-1\rangle$ then H contains a reflection and so $HQ = D_n$ if and only if $r \in HQ$. From Corollaries 1 and 2, we see that $r \in HQ$ if and only if the subgroups $\mathrm{ZDiv_n}(a-1)$ and $\langle a-1\rangle$ in $\mathbb{Z}_n$ have relatively prime generators. This last condition is clearly equivalent to both (2) and (3). QED

Example 1. Let $G = D_{36}$. We illustrate Theorem 2 and its corollaries for three different automorphisms of D_{36}. First, consider the automorphism $\theta_1 = 19x + 18$. Note that θ_1 is an involution. Applying Theorem 2 yields that for θ_1, $H = H_1 = \{1, r^2, r^4, \ldots, r^{34}, rs, r^3 s, \ldots, r^{35}s\}$ and $Q = Q_1 = \{1, r^{18}\}$,

which gives that $H_1 \cap Q_1 = \{1, r^{18}\} = Q_1$. Observe that $H_1Q_1 \neq D_{36}$, which is consistent with Corollary 3.

Now consider $\theta_2 = 5x+2$ which is an automorphism of order 6. In this case, $H_2 = \{1, r^9, r^{18}, r^{27}\}$ and $Q_2 = \{1, r^2, r^4, \ldots, r^{34}\}$. Thus, $H_2 \cap Q_2 = \{1, r^{18}\}$ and $H_2Q_2 \neq D_{36}$. However, in this case the inequality occurs because $2 \notin \langle 4\rangle \leq \mathbb{Z}_{36}$. Notice that even though this is a situation where $b \notin \langle a-1\rangle$, Q is still a subgroup of G, showing this can be the case.

Finally, consider the automorphism $\theta_3 = 5x + 4$ of D_{36}. This is also an automorphism of order 6. In this case, $H_3 = \{1, r^9, r^{18}, r^{27}, r^8s, r^{17}s, r^{26}s, r^{35}s\}$ and $Q_3 = \{1, r^4, r^8, r^{12}, \ldots, r^{32}\}$. Thus, $H_3 \cap Q_3 = \{1\}$ and this agrees with Corollary 3 since $r^9r^{28} = r$ and so $H_3Q_3 = D_{36}$.

From Theorem 2, we see that H is the disjoint union of $\{r^k \mid k(a-1) \equiv 0 \pmod n\}$ and $\{r^ks \mid k(a-1) \equiv -b \pmod n\}$. Notice that the second set may be empty if there is no solution, i, to the equation $i(a-1) \equiv -b \pmod n$ for fixed a and b (i.e. if $b \notin \langle a-1\rangle$). In fact, the two possibilities for the H-orbits on Q are determined by the existence of such a solution.

Proposition 5. *Let $G = D_n$ and $\theta = ax + b \in \mathrm{Aut}_k(D_n)$ for some k.*

(1) If $b \notin \langle a-1\rangle$, then the H-orbits on Q are:

$$H\backslash Q = \left\{\{r^j\} \mid j \in \langle a-1\rangle \cup (-b + \langle a-1\rangle)\right\}.$$

(2) If $b \in \langle a-1\rangle$, then the H-orbits on Q are:

$$H\backslash Q = \left\{\{r^j, r^{-j}\} \mid j \in \langle a-1\rangle\right\},$$

where $\langle a-1\rangle \leq \mathbb{Z}_n$. In either situation $G\backslash Q = \{Q\}$, i.e. there is a single G-orbit on Q.

Proof. Since H is fixed by θ, the action of H on Q is simply by conjugation. We note that $Q \subseteq \langle r\rangle \leq D_n$ and so we only need to describe the action of H on a general element, r^j. Then, let $r^i \in \{r^k \mid k(a-1) \equiv 0 \pmod n\} \subseteq H$. We see $r^ir^jr^{-i} = r^j$ so $\langle r\rangle$ fixes Q pointwise. Now suppose $r^is \in \{r^ks \mid k(a-1) \equiv -b \pmod n\} \subseteq H$. We have $r^isr^j(r^is)^{-1} = r^{-j}$ and so r^is takes r^j to r^{-j}. The result now follows since we will have $\{r^j, r^{-j}\}$ as an orbit if and only if there is $r^is \in H$, which is true if and only if $b \in \langle a-1\rangle$.

Finally, we demonstrate that every element of Q is in the G-orbit of $1 \in Q$. Notice that every element of Q is either of the form $q_1 = r^{p(a-1)} \in Q$ or $q_2 = r^{-b+p(a-1)} \in Q$. We have $r^{-p} \in G$ and $r^{-p}1\theta(r^{-p})^{-1} = r^{p(a-1)} = q_1$. Additionally, we have $r^{-p}s \in G$ and $r^{-p}s1\theta(r^{-p}s)^{-1} = r^{-p}r^{ap-b} = r^{-b+p(a-1)} = q_2$. Therefore, for any $q \in Q$, we can find $g \in G$ such that $g1\theta(g)^{-1} = q$ and so $G * 1 = Q$. Hence $G\backslash Q = \{Q\}$. QED

Example 2. Revisiting θ_1, θ_2, and θ_3 of Example 1, we apply Proposition 5 to obtain that for θ_1, since $18 \in \langle 18 \rangle$ and $r^{18} = r^{-18} \in D_{36}$,

$$H_1 \backslash Q_1 = \{\{1\}, \{r^{18}\}\};$$

for θ_2, since $2 \notin \langle 4 \rangle$,

$$H_2 \backslash Q_2 = \{\{1\}, \{r^2\}, \{r^4\}, \ldots, \{r^{34}\}\};$$

lastly, for θ_3, since $4 \in \langle 4 \rangle$,

$$H_3 \backslash Q_3 = \{\{1\}, \{r^4, r^{-4}\}, \{r^8, r^{-8}\}, \ldots, \{r^{32}, r^{-32}\}\}.$$

All of the results in this section hold for an automorphism of arbitrary finite order k, but in the next section we demonstrate that we can say more when we restrict our attention to $k = 2$, the involutions. In Section 5, we describe which of these results hold in the infinite dihedral group.

4 Involutions in $\mathrm{Aut}(D_n)$

In this section, we utilize the results from Sections 2 and 3 and expand on them in the situation when θ is an involution in $\mathrm{Aut}(D_n)$. For this entire section, we assume that $\theta = ax + b \in \mathrm{Aut}(D_n)$ and $\theta^2 = \mathsf{id}$. In particular, Proposition 1 forces $a \in \mathcal{R}_n^2$ and $b \in \mathrm{ZDiv_n}(a+1)$, i.e. $(a+1)b \equiv 0 \pmod{n}$. Recall that $\mathrm{Aut}_2(D_n) := \{\theta \in \mathrm{Aut}(D_n) \mid \theta^2 = \mathsf{id}\}$ is the collection of involutions (which includes the identity automorphism).

For our discussion of the involutions in $\mathrm{Aut}(D_n)$, it is necessary to understand the structure of $\mathcal{R}_n^2$, the square roots of unity in $\mathbb{Z}_n$. The following results can be found in an elementary number theory text (e.g. [7, Example 3.18]) but we include them here for completeness and for the usefulness of the proof.

Theorem 3. *Suppose that $n \geq 1$ and $n = 2^m p_1^{r_1} \cdots p_k^{r_k}$ where the p_i are distinct odd primes. Then,*

$$|\mathcal{R}_n^2| = \begin{cases} 2^k & \text{if } m = 0, 1 \\ 2^{k+1} & \text{if } m = 2 \\ 2^{k+2} & \text{if } m \geq 3. \end{cases}$$

Remark 2. We include the proof of Theorem 3 in the appendix (Section 7) because it demonstrates exactly how to construct the square roots of unity in $\mathbb{Z}_n$ provided we have the prime factorization of n. The construction only involves the Euclidean Algorithm and a map provided by the Chinese Remainder Theorem.

One can use the procedure described in the proof to effectively compute the square roots of unity in $\mathbb{Z}_n$ for any n. The construction of the square roots of unity provided in the appendix also provides the understanding necessary for Corollary 5 below.

The following corollary is the statement of Proposition 2 for involutions.

Corollary 4. *For any $n \geq 3$,*

$$|\operatorname{Aut}_2(D_n)| = \sum_{a \in \mathcal{R}_n^2} \gcd(a+1, n).$$

Remark 3. Corollary 4 together with the proof of Theorem 3 (see Remark 2) gives an easy way to compute the total number of involutions in $\operatorname{Aut}(D_n)$. Figure 1 provides a graph of the number of involutions in D_n for $n \leq 200$. This plot was generated using Sage [8].

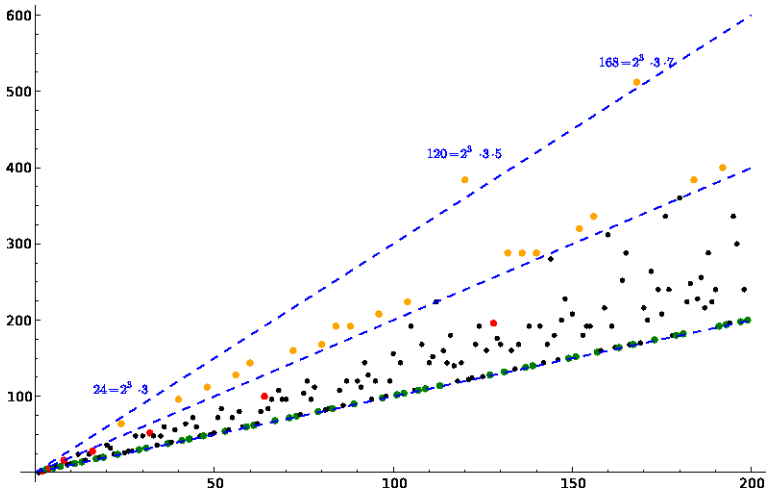

Figure 1. The number of involutions in $\operatorname{Aut}(D_n)$ for $n \leq 200$. The dashed lines represent the lines with slope 1, 2, and 3. The green dots represent primes, the red dots are powers of 2, and the yellow dots represent numbers n where the number of involutions is more than twice n.

Moreover, we can use Corollary 4 to provide a closed formula for the number of involutions.

Theorem 4. *Let $n \geq 3$ with $n = 2^m p_1^{r_1} \cdots p_k^{r_k}$ where the p_i are distinct odd*

primes. Then

$$|\operatorname{Aut}_2(D_n)| = \begin{cases} \prod_{i=1}^{k}(p_i^{r_i}+1) & \text{if } m=0, \\ 2\cdot\prod_{i=1}^{k}(p_i^{r_i}+1) & \text{if } m=1, \\ 6\cdot\prod_{i=1}^{k}(p_i^{r_i}+1) & \text{if } m=2, \\ (4+2^{m-1}+2^m)\cdot\prod_{i=1}^{k}(p_i^{r_i}+1) & \text{if } m\geq 3. \end{cases}$$

Proof. Let $\operatorname{inv}(n) = |\{z \in \operatorname{Aff}(\mathbb{Z}_n) \mid z^2 = \mathrm{id}\}|$; note that we then have $\operatorname{inv}(n) = |\operatorname{Aut}_2(D_n)|$ when $n \geq 3$. Next, suppose c and d are relatively prime and $n = c \cdot d$. Since $\mathbb{Z}_n \cong \mathbb{Z}_c \times \mathbb{Z}_d$ and $U_n \cong U_c \times U_d$, we have $\operatorname{Aff}(\mathbb{Z}_n) \cong \operatorname{Aff}(\mathbb{Z}_c) \times \operatorname{Aff}(\mathbb{Z}_d)$, and so $\operatorname{inv}(n) = \operatorname{inv}(c) \cdot \operatorname{inv}(d)$. Now, using Corollary 4 along with the the proof of Theorem 3, we get $\operatorname{inv}(2) = 2$, $\operatorname{inv}(4) = 2+4$, $\operatorname{inv}(2^m) = 2 + 2^{m-1} + 2 + 2^m$ for $m \geq 3$, and $\operatorname{inv}(p^r) = p^r + 1$ for p an odd prime. QED

Now we proceed to determine the equivalence classes of involutions. Let $\theta_1 = ax + b$ and $\theta_2 = cx + d$. We know from Proposition 3 that if $\theta_1 \sim \theta_2$, then $a = c$. Thus, to determine the equivalence classes of involutions it suffices to fix an $a \in \mathcal{R}_n^2$ and determine when $ax + b \sim ax + d$. Furthermore, according to Proposition 4, with a fixed, we simply need to describe the action of U_n on $\operatorname{ZDiv_n}(a+1)/\langle a-1\rangle$ in order to describe all the equivalence classes.

Recall that we denote the equivalence class of an involution θ by $\overline{\theta}$ and the number of equivalence classes with fixed leading coefficient a by:

$$N_a := \left|\left\{\overline{\theta} \mid \theta = ax + b \in \operatorname{Aut}_2(D_n)\right\}\right|.$$

Theorem 5. *Let $a \in \mathcal{R}_n^2$. The following hold.*

(1) $\langle a-1\rangle \leq \operatorname{ZDiv_n}(a+1)$ *and* $|\operatorname{ZDiv_n}(a+1)/\langle a-1\rangle| \leq 2$.

(2) $N_a = |\operatorname{ZDiv_n}(a+1)/\langle a-1\rangle| \leq 2$.

(3) $N_a = 2$ *if and only if* $n = 2^m \cdot y$ *where* $y \geq 1$ *is odd,* $m > 0$, *and* $a \equiv \pm 1 \pmod{2^m}$.

Proof. The first part of (1) is simply a restatement of Proposition 4 part (1). Now, suppose that $|\operatorname{ZDiv_n}(a+1)/\langle a-1\rangle| = j$. It is well known that $|\langle a-1\rangle| = \frac{n}{\gcd(a-1,n)}$ and we have already observed that $|\operatorname{ZDiv_n}(a+1)| = \gcd(a+1,n)$. Thus we have that $\frac{\gcd(a+1,n)}{\frac{n}{\gcd(a-1,n)}} = j$, or $\gcd(a+1,n)\gcd(a-1,n) = jn$. Now, suppose that

$$n = 2^m p_1^{r_1} \cdots p_k^{r_k}$$

with $m \geq 0$, the p_i distinct odd prime factors of n, and $r_i \geq 1$. Then, we must have that

$$\gcd(a+1,n) = 2^{m'} p_1^{s_1} \cdots p_k^{s_k} \text{ with } m' \leq m \text{ and } 0 \leq s_i \leq r_i \text{ for all } i, \text{ and}$$

$$\gcd(a-1,n) = 2^{m''} p_1^{t_1} \cdots p_k^{t_k} \text{ with } m'' \leq m \text{ and } 0 \leq t_i \leq r_i \text{ for all } i.$$

Now, we note that for all $i \in \{1, ..., k\}$ either $s_i = 0$ or $t_i = 0$. Indeed, if $s_i > 0$ and $t_i > 0$ then p_i divides both $a-1$ and $a+1$ which is impossible (since $p_i > 2$). Similarly, either $m' \leq 1$ or $m'' \leq 1$; otherwise, $2^{\min\{m',m''\}}$ divides $a-1$ and $a+1$ which is impossible.

Since $\gcd(a+1,n)\gcd(a-1,n) = jn$, we have that

$$2^{m'+m''} p_1^{s_1+t_1} \cdots p_k^{s_k+t_k} = j 2^m p_1^{r_1} \cdots p_k^{r_k}.$$

Now, since for all i either $t_i = 0$ or $s_i = 0$, we necessarily have $s_i + t_i = r_i$. Dividing out, we get $2^{m'+m''} = j2^m$. We also know that $m' \leq m$ and $m'' \leq m$ and since either $m' \leq 1$ or $m'' \leq 1$, we have $m \leq m' + m'' \leq m+1$. Dividing out we have $j = 2^{m'+m''-m}$ and so $1 \leq j \leq 2$ as required for Claim (1).

Now, by to Theorem 1, N_a is the number of divisors of $\frac{\gcd(a-1,n)\gcd(a+1,n)}{n}$, and thus N_a is the number of divisors of j computed above. Therefore, $N_a = 1$ if $j = 1$ and $N_a = 2$ if $j = 2$. In either case, $N_a = |\mathrm{ZDiv_n}(a+1)/\langle a-1\rangle| \leq 2$ proving Claim (2).

Finally, according to the proof of (1), we have $j = 2$ if and only if $m' = 1$ and $m'' = m$ or $m' = m$ and $m'' = 1$. In the first case, we have that 2^m divides $a-1$, and in the second case we have that 2^m divides $a+1$. Therefore, $a \equiv \pm 1 \pmod{2^m}$. QED

Theorem 5, Theorem 3 and Remark 2 combined together allow us to compute the number of distinct equivalence classes of involutions in $\mathrm{Aut}_2(D_n)$ for fixed n if we have the prime factorization of n. In fact, we get a closed formula for the number of equivalence classes of elements in $\mathrm{Aut}_2(D_n)$ as follows.

Corollary 5. *Suppose that $n \geq 3$ and $n = 2^m p_1^{r_1} \cdots p_k^{r_k}$ where the p_i are distinct odd primes. Then, the number of equivalence classes, C_n, of $\mathrm{Aut}_2(D_n)$ is given by*

$$C_n = \begin{cases} 2^k & \text{if } m = 0 \\ 2^{k+1} & \text{if } m = 1 \\ 2^{k+2} & \text{if } m = 2 \\ 2^{k+3} - 2^{k+1} & \text{if } m \geq 3. \end{cases}$$

See Figure 2 for a plot of these numbers.

Proof. According to Theorem 5, we know N_a for every $a \in \mathcal{R}_n^2$. When $m = 0$, n is odd and we know that $N_a = 1$ for all a. Thus, there is one equivalence class for every element of $\mathcal{R}_n^2$ proving the first formula. If $m = 1, 2$, then every $a \in \mathcal{R}_n^2$

is odd and so satisfies $a \equiv \pm 1 \pmod{m}$. Thus for every element $a \in \mathcal{R}_n^2$, we get two equivalence classes for a total of $2 \cdot |\mathcal{R}_n^2|$ equivalence classes. Finally, when $m \geq 3$, using the construction of the elements of $\mathcal{R}_n^2$ found in the proof in the appendix, we see that exactly half of these elements satisfy the condition $a \equiv \pm 1 \pmod{m}$. Therefore, for half the elements in $\mathcal{R}_n^2$ we have $N_a = 1$ and for the other half we have $N_a = 2$ giving us a total of $2^{k+2} + (2^{k+2} - \frac{1}{2} \cdot 2^{k+2}) = 2^{k+3} - 2^{k+1}$ equivalence classes, proving the result. QED

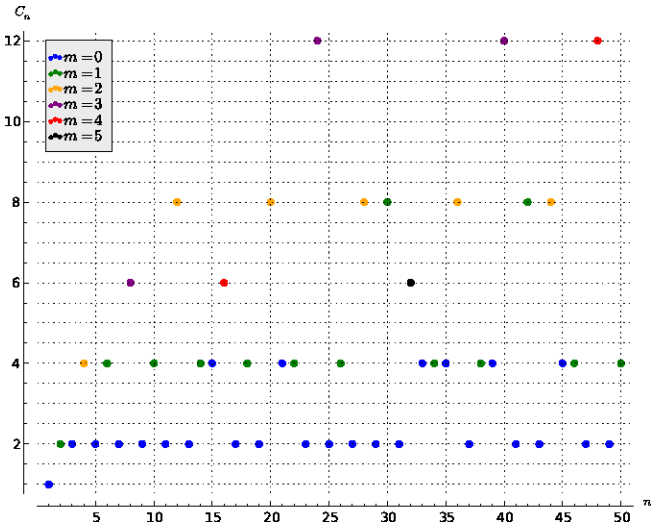

Figure 2. Number of equivalence classes of involutions in $\mathrm{Aut}(D_n)$ vs. n for $n \leq 50$.

Remark 4. According to the Online Encyclopedia of Integer Sequences, the sequence described in Corollary 5 also counts the number (up to isomorphism) of groups of order $2n$ that have a subgroup isomorphic to $\mathbb{Z}_n$ [1]. To be more precise, we include a brief discussion of the natural bijection between these two objects. Suppose $\theta = ax + b$ is an involution. Then $w_a : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n) = U_n$ given by $w_a(0) = 1$ and $w_a(1) = -a$ is an injective homomorphism and induces a $\mathbb{Z}_2$-action on $\mathbb{Z}_n$. Next, we define $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_n$ by $f(c, d) = 0$ if $c = 0$ or $d = 0$ and $f(1, 1) = b$; it is easily shown that f is a 2-cocycle if and only if $b \in \mathrm{ZDiv_n}(a + 1)$. Finally, it is well known (see [10, Chapter 6.6])) that 2-cocyles give rise to group extensions and two different 2-cocycles give isomorphic group extensions if they are cohomologous. A simple calculation shows that if $\theta = ax+b$ and $\theta' = ax + b'$, then the corresponding 2-cocycles are cohomologous if and only if $b - b' \in \langle a - 1 \rangle$, which matches the characterization of automorphisms being equivalent above.

We now use our previous results from Section 3 to fully describe the sets H_θ and Q_θ when θ is an involution; moreover, in this situation, we are also interested in the set of twisted involutions

$$R = R_\theta = \{x \in G \mid \theta(x) = x^{-1}\}.$$

A quick calculation gives

$$R = \{r^k \mid k \in \mathrm{ZDiv_n}(a+1)\} \cup \{r^k s \mid k(a-1) \equiv -b \pmod{n}\}. \tag{3}$$

Using the results from Theorem 2 we describe Q and $R - Q$.

Corollary 6. *If $\theta = ax + b$ is an involution, then Q is a subgroup of $\langle r \rangle$ and under the natural isomorphism $\psi : \langle r \rangle \xrightarrow{\cong} \mathbb{Z}_n$ we have*

$$\psi(Q) = \begin{cases} \langle a-1 \rangle, & \text{if} \quad b \in \langle a-1 \rangle \\ \mathrm{ZDiv_n}(a+1), & \text{otherwise.} \end{cases}$$

Furthermore, $R - Q = \{r^k \mid k \in \mathrm{ZDiv_n}(a+1) \setminus \langle a-1 \rangle\} \cup \{r^k s \mid k(a-1) \equiv -b \pmod{n}\}$

Proof. We proceed using Theorem 2 and applying Theorem 5. Indeed, by Theorem 2 $\psi(Q)$ consists of the union of the two cosets $\langle a-1 \rangle$ and $-b + \langle a-1 \rangle$. These cosets are the same if $-b \in \langle a-1 \rangle$ (which means $b \in \langle a-1 \rangle$) and then $\psi(Q) = \langle a-1 \rangle \leq \mathrm{ZDiv_n}(a+1)$, or they are distinct and by Theorem 5 part (1) there are only 2 cosets total so $\langle a-1 \rangle \cup (-b + \langle a-1 \rangle) = \mathrm{ZDiv_n}(a+1)$. In either case, Q is a subgroup of $\langle r \rangle$ and $\psi(Q)$ is as described in the statement of the corollary. Finally, the result about $R - Q$ is immediate from equation (3). QED

Corollary 7. *If $b \notin \langle a-1 \rangle$ then $R = Q$.*

Remark 5. We note that due to Theorem 5, $\psi(Q)$ given in Corollary 6 is almost always $\mathrm{ZDiv_n}(a+1)$ for involutions. The only instance where $\psi(Q) \neq \mathrm{ZDiv_n}(a+1)$ occurs when $|\mathrm{ZDiv_n}(a+1)/\langle a-1 \rangle| = 2$ and $b \in \langle a-1 \rangle$. We revisit $\theta_1 = 19x + 18$ from Example 1, which is an involution, noting that this is in fact a case where $b \in \langle a-1 \rangle$. Recalling that $Q_1 = \{1, r^{18}\}$, we see that $\psi(Q_1)$ is indeed isomorphic to $\langle a-1 \rangle = \langle 18 \rangle < \mathbb{Z}_{36}$. We also have that $R = R_1 = \{1, r^9, r^{18}, r^{27}, rs, r^3s, r^5s, \ldots r^{33}s, r^{35}s\}$, and thus $R_1 - Q_1 = \{r^9, rs, r^3s, r^5s, \ldots, r^{35}s\}$.

In the setting of algebraic groups, the symmetric space Q is almost never a subgroup; this follows from the fact that if G is an algebraic group, then an involution would split the Lie algebra $\mathfrak{g}$ of G into a direct sum of eigenspaces,

say $\mathfrak{g} = \mathfrak{h} + \mathfrak{q}$, where $\mathfrak{q}$ is the Lie algebra of Q. Since $[\mathfrak{q}, \mathfrak{q}] \subseteq \mathfrak{h}$, then $\mathfrak{q}$ will not be a Lie subalgebra of $\mathfrak{g}$ unless it is abelian. Thus, Corollary 6 is interesting since here Q is always a subgroup. It would also be interesting to determine if this holds in other finite groups or if it is a special property of dihedral groups.

Furthermore, in the setting of algebraic groups, it is known for involutions θ_1 and θ_2 that $\theta_1 \sim \theta_2$ if and only if $H_{\theta_1} \cong H_{\theta_2}$ (see [4]). Now we show that this result does not hold for finite groups.

Corollary 8. *There exists n and involutions $\theta_1, \theta_2 \in \mathrm{Aut}(D_n)$ such that $H_{\theta_1} = H_{\theta_2}$ but $\theta_1 \not\sim \theta_2$.*

Proof. Let $n = 8$ and $\theta_1 = 7x$ and $\theta_2 = 3x$. According to Proposition 3, $\theta_1 \not\sim \theta_2$ because $7 \neq 3$ (in U_8). However, according to Theorem 2, $H_{\theta_1} = \{1, r^4, s, r^4 s\}$ and $H_{\theta_2} = \{1, r^4, s, r^4 s\}$. QED

5 The Infinite Dihedral Group D_∞

So far we have discussed the finite dihedral groups D_n. However, it turns out that there are similar results for the infinite dihedral group

$$D_\infty = \langle r, s \mid s^2 = 1,\ rs = sr^{-1} \rangle.$$

In this case, the automorphisms are the affine linear transformations of $\mathbb{Z}$, so are of the form $ax + b$ where $b \in \mathbb{Z}$ and $a \in \{\pm 1\}$. Then, the congruences given in equation (1) become equations over the integers. In particular, it easy to show that the only automorphisms of finite order, besides the identity, are the involutions and they have the form $-x + b$ where $b \in \mathbb{Z}$.

Proposition 6. *The following hold:*

(1) If $\theta \in \mathrm{Aut}(D_\infty)$ has finite order, then $\theta = x$ or $\theta = -x + b$ for some integer b.

(2) $-x + b \sim -x + d$ if and only if $b \equiv d \pmod 2$.

Proof. Part (1) follows from the equations (1) given in the proof of Proposition 1. For part (2), observe that an argument analogous to the one given in the proof of Proposition 3 can be used here with $\mathbb{Z}$ in place of $\mathbb{Z}_n$ and $\{1, -1\}$ in place of U_n. QED

We see that in D_∞ the situation is simple: the only automorphisms of finite order are involutions (including the identity) and there are only two distinct equivalence classes of non-identity involutions represented by $\chi_0 = -x = \mathrm{conj}(s)$

(inner) and $\chi_1 = -x+1$ (outer). Note that χ_1 represents the class of the diagram automorphism discussed in Section 1.

The fixed-point subgroup and symmetric space of an involution $\theta = \chi_i$ is similarly easy to compute.

$$\begin{array}{lll} H_{\chi_0} = \{1, s\}, & Q_{\chi_0} = \langle r^2 \rangle, & R_{\chi_0} = \langle r \rangle \cup \{s\} \\ H_{\chi_1} = \{1\}, & Q_{\chi_1} = \langle r \rangle, & R_{\chi_1} = \langle r \rangle. \end{array} \tag{4}$$

We note that the descriptions in equation (4) show that Corollary 6 holds in the infinite case as well. However, in this case, the description is simpler because the description of Q depends only on whether b is even or odd. We also note that despite the fact that the two cases are different when viewing Q as a subgroup of D_∞, we always have $Q \cong \mathbb{Z}$.

6 Acknowledgements

The authors thank the American Institute of Mathematics in Palo Alto, CA for its generous support. We also thank the referees for helpful comments.

7 Appendix: Proof of Theorem 3

Proof. Our goal is to determine the size of $|\mathcal{R}_n^2|$ for all n. First, suppose that $n = p^r$ where p is an odd prime and $r \geq 1$. Then, suppose $a \in \mathbb{Z}_{p^r}$ and that $a^2 - 1 \equiv 0 \pmod{p^r}$. Then we have that $(a+1)(a-1) \equiv 0 \pmod{p^r}$ and so $(a+1)(a-1) = kp^r$ for some $k \in \mathbb{Z}$. Since p is an odd prime, it is clear that p cannot divide both $a+1$ and $a-1$; it follows that p^r divides $a+1$ or p^r divides $a-1$. So $a = 1$ or $a = p^r - 1$, thus $|\mathcal{R}_{p^r}^2| = 2$. Next, it is clear that $|\mathcal{R}_2^2| = 1$ and $|\mathcal{R}_4^2| = 2$. Suppose that $n = 2^m$ with $m \geq 3$. Since 1 and $n-1$ are always square roots of unity mod n, we only consider other numbers a with $a^2 \equiv 1 \pmod{n}$. Since n is even, we must have that a is odd, so assume that $a = 2k+1$ for some $0 \leq k \leq 2^{m-1}$. Then $1 \equiv a^2 \equiv (2k+1)^2 \equiv 4k^2 + 4k + 1 \pmod{n}$ so that $4k(k+1) = l \cdot 2^m$ for some $l \geq 1$. In particular, since $m \geq 3$, we have $k(k+1) = l \cdot 2^{m-2}$ for some m. Either k or $k+1$ is odd and thus cannot divide 2^{m-2}.

Case 1: k is even. So $k = h \cdot 2^{m-2}$ for some $1 \leq h \leq 2$ (since $k \leq 2^{m-1}$). Then, if $h = 1$, $a = 2^{m-1} + 1$. If $h = 2$, then $a \equiv 1 \pmod{n}$.

Case 2: k is odd. So $k+1$ is even and $k+1 = h \cdot 2^{m-2}$ with $1 \leq h \leq 2$. Then, if $h = 1$, $a = 2^{m-1} - 1$. If $h = 2$, then $a = 2^m - 1 \equiv n - 1 \pmod{n}$.

So, there are four possibilities for a: $1, n-1, 2^{m-1}+1, 2^{m-1}-1$. It is easy to check that these are all in fact square roots of 1, showing that $|\mathcal{R}^2_{2^m}| = 4$ if $m \geq 3$.

Finally, the result holds due to the fact that the Chinese Remainder Theorem guarantees that if $n = 2^m p_1^{r_1} \cdots p_k^{r_k}$ then

$$\mathbb{Z}_n \cong \mathbb{Z}_{2^m} \times \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}.$$

Then, it is clear that any square root of $(1, ..., 1)$ (the identity from the right hand side) must be of the form $(a_0, a_1, ..., a_k)$ where $a_0 \in \mathcal{R}^2_{2^m}$ and $a_i \in \mathcal{R}^n_{p_i^{r_i}}$ for $i \in \{1, ..., k\}$. We have counted the possibilities for a_i above and so we can multiply these together to get all the possible choices for $a \in \mathbb{Z}_n$ with $a^2 \equiv 1 \pmod{n}$. In particular, we get $|\mathcal{R}^2_n| = 2^k$ if $m \in \{0, 1\}$, $|\mathcal{R}^2_n| = 2 \cdot 2^k$ if $m = 2$ and $|\mathcal{R}^2_n| = 2^2 \cdot 2^k$ if $m \geq 3$ as required. QED

References

[1] OEIS Foundation Inc. (2012), The On-Line Encyclopedia of Integer Sequences, http://oeis.org/A147848.

[2] Anders Björner, Francesco Brenti: *Combinatorics of Coxeter groups*, Graduate Texts in Mathematics, vol. 231, Springer, New York, 2005.

[3] Nicolas Bourbaki: *Lie groups and Lie algebras. Chapters 4–6*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 2002, Translated from the 1968 French original by Andrew Pressley.

[4] A. G. Helminck, S. P. Wang, *On rationality properties of involutions of reductive groups*, Adv. in Math. **99** (1993), 26–96.

[5] A.G. Helminck: *Symmetric k-varieties*, Proc. Sympos. Pure Math. **56** (1994), no. 1, 233–279.

[6] James E. Humphreys: *Reflection groups and Coxeter groups*, Cambridge Studies in Advanced Mathematics, vol. 29, Cambridge University Press, Cambridge, 1990.

[7] Gareth A. Jones, J. Mary Jones: *Elementary number theory*, Springer Undergraduate Mathematics Series, Springer-Verlag London Ltd., London, 1998.

[8] W. A. Stein et al.: *Sage Mathematics Software (Version 4.8)*, The Sage Development Team, 2012, `http://www.sagemath.org`.

[9] Gary L. Walls: *Automorphism groups*, Amer. Math. Monthly **93** (1986), no. 6, 459–462.

[10] Charles A. Weibel: *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38 , Cambridge University Press, Cambridge, 1994.